

### **REMARKS**

This amendment is filed in response to the Office action mailed August 16, 2010.  
All rejections and objections are respectfully traversed.

Claims 3 – 13, 15, 17 – 19 and 27 – 29 are pending in this case.

No new claims have been added.

### **Interview Summary**

On October 28, 2010, the Applicant's Attorney conducted a telephone interview with the Examiner. The Examiner stated that he would issue a Supplemental Office Action because specific arguments in the previous amendment were not addressed. As of yet, no Supplemental Office Action has been mailed. As such, the Applicant's Attorney was forced to file this amendment to preserve the Applicant's rights.

### **Claim Rejection – 35 USC §103**

At pages 3 – 9 of the Office Action, claims 27 – 29 were rejected under 35 U.S.C. §103(a) over Uchishiba et al., U.S. Publication No. 2002/0116812 (hereinafter “Uchishiba”), in view of Kazar et al., U.S. Patent No. 6,868,417 (hereinafter “Kazar”), in further view of Shu et al., U.S. Patent No. 7,555,772 (hereinafter “Shu”), in further view of Saraiya et al., U.S. patent No. 7,685,281 (hereinafter “Saraiya”).

Applicant's claimed invention, as set forth by new independent claim 27, recites:

27. A system comprising:  
a processor;  
a memory coupled to the processor;  
a storage operating system resident in the memory and executed by the processor, the storage operating system implementing a file system configured to provide storage service of information stored on the system;  
a plurality of network interfaces configured to process received block-based protocol data access requests, each network interface assigned to one or more network addresses, each network interface further assigned an identifier that binds the network interface to an address space that includes the one or more network addresses; and  
*a plurality of context data structures stored in the memory and containing configuration information to establish a plurality of instances of virtual servers executed by the processor, each virtual server allocated resources that include a partitioning of the network interfaces*

*and assigned network addresses to establish a distinct security domain for that virtual server that enables controlled access to the allocated network interfaces and assigned network addresses, each virtual server further configured to share access to the file system to service the block-based protocol data access requests by converting the block-based protocol data access requests to appropriate file system data requests when providing the storage service of the information stored on the system.*

The Applicant respectfully submits that a combination of Uchishiba, Kazar, Shu, and Saraiya does not teach or suggest the Applicant's claimed "*a plurality of context data structures stored in the memory and containing configuration information to establish a plurality of instances of virtual servers executed by the processor, each virtual server allocated resources that include a partitioning of the network interfaces and assigned network addresses to establish a distinct security domain for that virtual server that enables controlled access to the allocated network interfaces and assigned network addresses, each virtual server further configured to share access to the file system to service the block-based protocol data access requests by converting the block-based protocol data access requests to appropriate file system data requests when providing the storage service of the information stored on the system.*"

The Applicant's claimed technique stores a plurality of context data structures containing configuration information to establish a plurality of instances of virtual servers. **Each vfiler is allocated resources that include a partitioning of network interfaces and assigned network addresses to establish a distinct security domain for that virtual server.** This allocation enables each virtual server to have controlled access to its allocated network interfaces and assigned network addresses. Further, the virtual servers **share access to the file system that services block-based protocol data access requests by converting the block-based protocol data access requests to appropriate file system data requests.**

As an illustrative example, consider the following. A context data structure of a first vfiler ensures that users or clients of a first security domain can use a first set network interfaces and network addresses (e.g., the allocated resources) when issuing requests to access a first subset of storage resources on a shared storage appliance.

Similarly, the context data structure of a second vfiler ensures that clients of a second security domain may use a second set of network interfaces and network addresses (e.g., the allocated resources), that are distinct from the allocated resources dedicated to the first vfiler, to access a second subset of storage resources. For example, the first vfiler may be allocated network addresses 1 – 10 and have access to the file system. Similarly, the second vfiler may be allocated network addresses 22 – 40 and also have access to the file system. Advantageously, clients associated with the first vfiler and the first security domain are unaware of the “presence” of the second vfiler and the second security domain. That is, each vfiler has its own dedicated context data structure that enables controlled access to the allocated resources that include a partitioning of network interfaces and assigned network addresses to establish a distinct security domain, while allowing the virtual servers to share access to the file system that services block-based protocol data access requests by converting the block-based protocol data access requests to appropriate file system data requests.

The Applicant notes that there appears to be agreement that Uchishiba and Saraiya do not address this aspect of the Applicant’s claims. *See* Office Action, pages 7 – 9.

Further, the Applicant respectfully submits that the deficiencies of Uchishiba and Saraiya are not remedied by a combination with Kazar. Instead, Kazar describes a technique “For handling file level and block level remote file accesses” using the same server. *See* Kazar, Abstract. Specifically, in describing a “block level service ... in terms of the inode layer operation”, Kazar states that “a block\_login operation passes in a user ID and a password, and authenticates the user for the service. Based upon the user, the server chooses a particular file system to which the user’s block read and write operations will be applied.” *See* Kazar, col. 9, line 64 – col. 10, line 1. Kazar makes no mention of allocating resources that include **a partitioning of network interfaces and assigned network addresses to each virtual server to establish a distinct security domain for that virtual server** to enable each virtual server controlled access to its allocated network interfaces and assigned network addresses. Further, Kazar makes no mention of virtual servers (that were each allocated network interfaces and assigned network

addresses) **sharing access to a file system to service the block-based protocol data access requests through conversion to appropriate file system data requests.** As such, the Applicant respectfully submits that Kazar may not fairly be interpreted to teach or suggest these aspects of the Applicant's claim.

Finally, Shu simply states that a firewall may be partitioned into multiple virtual systems, where each virtual system is a unique security domain and can be managed by administrators who may individualize security protection for the domain. *See* Shu, col. 8, lines 55 – 62. The “virtual systems” (that are a partition of a firewall) as described in Shu are not akin to the Applicant's claimed virtual servers. Specifically, Shu's “virtual systems” are not allocated resources that include **a partitioning of network interfaces and assigned network addresses to each virtual server to establish a distinct security domain for that virtual server** to enable each virtual server controlled access to its allocated network interfaces and assigned network addresses. Instead, Shu's “virtual systems” as simply partitions of a firewall. Further, Shu's “virtual systems”, that are partitions of a firewall, do not **share access to a file system to service the block-based protocol data access requests through conversion to appropriate file system data requests.** . As such, the Applicant respectfully submits that Shu may not fairly be interpreted to teach or suggest these aspects of the Applicant's claim.

Accordingly, Applicant respectfully urges that a combination of Uchishiba, Kazar, Shu, and Saraiya is legally insufficient to render the present claims unpatentable under 35 U.S.C. 103(a) because of the Absence of the Applicant's claimed ***“a plurality of context data structures stored in the memory and containing configuration information to establish a plurality of instances of virtual servers executed by the processor, each virtual server allocated resources that include a partitioning of the network interfaces and assigned network addresses to establish a distinct security domain for that virtual server that enables controlled access to the allocated network interfaces and assigned network addresses, each virtual server further configured to share access to the file system to service the block-based protocol data access requests by converting the block-based protocol data access requests to appropriate file system data requests when providing the storage service of the information stored on the system.”***

At pages 9 – 13 of the Office Action, claim 3, 6, 12 – 13, 15, and 17 were rejected under 35 U.S.C. §103(a) over Uchishiba, in view of Kazar, in further view of Shu, in further view of Saraiya, and in further view of Becker-Szendy et al., U.S. Patent No. 7,243,089 (hereinafter “Becker-Szendy”).

At pages 13 – 15 of the Office Action, claims 4 – 5 and 18 – 19 were rejected under 35 U.S.C. §103(a) over Uchishiba, in view of Kazar, in further view of Shu, in further view of Saraiya, in further view of Becker-Szendy, and in further view of Mane et al., U.S. Publication No. 2005/0050107 (hereinafter “Mane”).

At pages 15 – 19 of the Office Action, claims 7 – 11 were rejected under 35 U.S.C. §103(a) over Uchishiba, in view of Kazar, in further view of Shu, in further view of Saraiya, and in further view of Becker-Szendy, and in further view of George et al., U.S. Patent No. 7,010,663 (hereinafter “George”).

The Applicant notes that claims 3 – 13, and 15, and 17 – 19 are dependent claims that depend from independent claims believed to be in condition for allowance. Accordingly, claims 3 – 13, and 15, and 17 – 19 are believed to be in condition for allowance due to their dependency, as well as for other separate reasons.

### ***Conclusion***

All independent claims are believed to be in condition for allowance.

All dependent claims are dependent from independent claims which are believed to be in condition for allowance. Accordingly, all dependent claims are believed to be in condition for allowance.

Favorable action is respectfully solicited.

Please charge any additional fee occasioned by this paper to our Deposit Account No. 03-1237.

Respectfully submitted,

/Omar M. Wadhwa/  
Omar M. Wadhwa  
Reg. No. 64,127  
CESARI AND MCKENNA, LLP  
88 BLACK FALCON AVENUE  
BOSTON, MA 02210  
Telephone: (617) 951-2500  
Facsimile: (617) 951-3927